AMENDMENTS TO THE CLAIMS

Please find below a complete listing of the claims in the application, including their status as effected by the present amendment:

1.– 34. (*previously cancelled*)

35. (*currently amended*) An authentication system, comprising:

an access controller operable to communicate with a client via a first communication medium; and

an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;

wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.

36. (*previously presented*) The authentication system according to claim 35, wherein said authentication server is operable to generate said first key and said second key.

37. (*previously presented*) The authentication system according to claim 35, wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

38. (*previously presented*) The authentication system according to claim 35, wherein each of said first communication medium and said second communication medium is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

39. (*currently amended*) The authentication system according to claim 35, wherein said computer is a telecommunications switch.

40. (*previously presented*) The authentication system according to claim 35, wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found.

41. (*previously presented*) The authentication system according to claim 35, wherein said instructions are encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instructions by said access controller using said second key.

42. (*previously presented*) The authentication system according to claim 35, wherein said first key is delivered to said client only after said second key has been successfully delivered to said access controller.

43. (*cancelled*)

44. (*currently amended*) The authentication system according to claim 35, wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

45. (*currently amended*) An access controller for intermediating communications between an interface and a computer and operable to store a second key complementary to a first key; said access controller operable to communicate with a client via said interface; said client operable to store said first key and to receive instructions from a user; said access controller operable to selectively pass said instructions to said computer if a verification protocol utilizing said keys is met;

wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found.

46. (*previously presented*) The access controller of claim 45, wherein said access controller is operable to obtain said second key from an authentication server and said client is operable to obtain said first key from said authentication server.

47. (*previously presented*) The access controller of claim 46, wherein said authentication server is operable to generate said first key and said second key.

48. (*previously presented*) The access controller of claim 45, wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

49. (*previously presented*) The access controller of claim 45, wherein a medium for connecting said interface and said client is selected from the group consisting of an RS-232 cable, a USB cable, the Internet, the PSTN, a local area network, and a wireless network.

50. (*previously presented*) The access controller of claim 45, wherein said computer is a telecommunications switch.

51. (*cancelled*)

52. (*previously presented*) The access controller of claim 45, wherein said instructions are encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instructions by said access controller using said second key.

53. (*previously presented*) The access controller of claim 46, wherein said first key is obtained by said client only after said second key has been successfully obtained by said access controller.

54. (*previously presented*) The access controller of claim 46, wherein said first key is obtained by said client only if a user operating said client authenticates said user's identity with said authentication server.

55. (*previously presented*) The access controller of claim 46, wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

56. (*previously presented*) In an authentication server, a method of securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing a set of keys is met, said method comprising:

receiving a request from said access controller for an updated first key;

authenticating said request;

determining said updated first key and a second key corresponding to said updated first key; and

delivering said updated first key to said access controller.

57. (*previously presented*) The method of claim 56, further comprising:

receiving a second request from said client for said second key;

authenticating said second request;

delivering said second key to said client.

58. (*previously presented*) The method according to claim 56, wherein determining said updated first key and said second key includes generating said updated first key and said second key.

59. (*previously presented*) The method according to claim 56, wherein said updated first key is a private encryption key and said second key is a public encryption key complementary to said private encryption key.

60. (*previously presented*) The method according to claim 56, wherein a communication medium between at least one of said authentication server, said access controller and said client is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

61. (*previously presented*) The method according to claim 56, wherein said computer is a telecommunications switch.

62. (*previously presented*) The method according to claim 56, wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said second key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted number using said updated first key by said access controller, a comparison of said random number and said decrypted number, and a decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found.

63. (*previously presented*) The method according to claim 56, wherein said instructions are encrypted by said client using said second key and said verification protocol is based on a successful decryption of said instructions by said access controller using said updated first key.

64. (*previously presented*) The method according to claim 57, wherein said second key is delivered to said client only after said updated first key has been verified as having been successfully delivered to said access controller.

65. (*previously presented*) The method according to claim 57, wherein said second key is delivered to said client only if a user operating said client authenticates said user's identity with said authentication server.

66. (*previously presented*) The method according to claim 57, wherein said access controller contains a preset first key and said authentication server maintains a record of said preset first key; said authentication server operable to deliver said updated first key and said second key only if said access controller successfully transmits said preset first key to said authentication server and said transmitted preset first key matches said authentication server's record thereof.

67. (*previously presented*) A method of securing access between a client and a computer having an access controller intermediate said client and said computer, said method comprising:

receiving an instruction at said client destined for said computer;

generating a random number by said client;

encrypting said random number by said client using a first key;

delivering said random number, said encrypted random number and said instruction to said access controller;

decrypting said encrypted random number using a second key by said access controller, said second key complementary to said first key;

comparing said random number and said decrypted number;

passing at least a portion of said instruction to said computer if said comparison finds a match of said random number with said decrypted number; and,

discarding said at least a portion if no match is found.

68. (*currently amended*) An authentication server, comprising:

an interface for communicating with a client and an access controller via a communication medium; and

a processing unit operable to determine a first key for delivery to said client and a second key for delivery to said access controller, said first key being delivered to said client only if a user operating said client authenticates said user's identity with said server; such that when said access controller and said client are connected, said access controller selectively passes instructions from said client to a computer attached to said access controller if a verification protocol utilizing said keys is met.

69. (*previously presented*) The authentication server of claim 68, wherein said processing unit is operable to generate said first key and said second key.

70. (*previously presented*) An authentication server for securing access between a client having temporary connection to a computer via an access controller, said access controller for selectively passing instructions received from said client to said computer if a verification protocol utilizing a set of keys is met, said authentication server comprising:

means for receiving a request from said access controller for an updated first key;

means for authenticating said request;

means for determining said updated first key and a second key corresponding to said updated first key; and,

means for delivering said updated first key to said access controller.

71. (*previously presented*) The authentication server of claim 70, wherein said means for determining said updated first key and said second key is operable to generate said updated first key and said second key.

72. (*previously presented*) In an access controller for selectively passing instructions between a client and a computer if a verification protocol is met, a method of expiring said verification protocol, comprising:

determining if a first preset period of time since said client disconnected from said access controller has elapsed;

determining if a second preset period of time since said verification protocol was updated has elapsed; and,

expiring said verification protocol by refusing to pass said instructions if either of said preset periods of time have elapsed.

73. (*previously presented*) The method according to claim 72, wherein said verification protocol utilizes a first encryption key respective to said client and a second encryption key respective to said access controller and said expiring step includes an instruction to said access controller to refuse to accept communications from said client that utilize said first encryption key.

74. (*new*) An authentication system, comprising:

an access controller operable to communicate with a client via a first communication medium; and

an authentication server operable to communicate with said client and said access controller via a second communication medium and further operable to deliver a first key to said client and a second key to said access controller, said second key being complementary to said first key such that when said client and said access controller are connected, communications therebetween can be encrypted using said keys; and wherein said access controller is operable to selectively pass instructions received from

said client to a computer attached to said access controller if a verification protocol utilizing said keys is met;

wherein said access controller contains a preset second key and said authentication server maintains a record of said preset second key; said authentication server operable to deliver said first key and said second key only if said access controller successfully transmits said preset second key to said authentication server and said transmitted preset second key matches said authentication server's record thereof.

75. (*new*) The authentication system according to claim 74, wherein said authentication server is operable to generate said first key and said second key.

76. (*new*) The authentication system according to claim 74, wherein said first key is a public encryption key and said second key is a private encryption key complementary to said public encryption key.

77. (*new*) The authentication system according to claim 74, wherein each of said first communication medium and said second communication medium is selected from the group of networks consisting of the Internet, the PSTN, a local area network, and a wireless network.

78. (*new*) The authentication system according to claim 74, wherein said computer is a telecommunications switch.

79. (*new*) The authentication system according to claim 74, wherein said verification protocol includes a generation of a random number by said client, an encryption of said random number by said client using said first key, a delivery of said random number and said encrypted random number from said client to said access controller, a decryption of said encrypted random number using said second key by said access controller, a comparison of said random number and said decrypted number, and a

decision to pass at least a portion of said instructions if said comparison finds a match of said random number with said decrypted number, and a decision not to pass said at least a portion of said instructions if no match is found.

80. (*new*) The authentication system according to claim 74, wherein said instructions are encrypted by said client using said first key and said verification protocol is based on a successful decryption of said instructions by said access controller using said second key.

81. (*new*) The authentication system according to claim 74, wherein said first key is delivered to said client only after said second key has been successfully delivered to said access controller.

82. (*new*) The authentication system according to claim 74, wherein said first key is delivered to said client only if a user operating said client authenticates said user's identity with said server.